UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,943	12/09/2003	William E. Freeman	149391	2711

38598 7590 01/15/2008

ANDREWS KURTH LLP
1350 I STREET, N.W.
SUITE 1100
WASHINGTON, DC 20005

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,943	FREEMAN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-9,11-23 and 25-27* is/are rejected.

7)☒ Claim(s) *10 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 11/06/07. Claims 1-16, 21 and 24 have been amended.

Response to Arguments

2. Applicant's arguments with respect to the rejection of claims 21-27 under 35 USC 101 as being directed to non-statutory subject matter have been fully considered but they are not persuasive. Applicant argues that the amended claims have overcome the rejection (page 7, paragraph 5). Although the amended claim recites "An apparatus comprising computing devices", none of the claimed elements is a physical part of a device (e.g., a processor, memory, etc.) can the apparatus as claimed constitute part of a device or a combination of devices to be a machine within the meaning of 101. Since all elements of the claim can be reasonably interpreted in light of the disclosure by one of ordinary skill as software routines (see page 8, lines 20-22), the claim is directed to software per se, which fails to fall within one of the four statutory classes of § 101.

3. Applicant's arguments with respect to the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Asanoma et al. (2003/0056099) in

view of Chen et al. (7,099,476) have been fully considered but they are not persuasive.

Applicant argues that Asanoma does not teach using multiple private keys by the smart card and that the private keys PRk1 and PRk2 shown in figure 9 merely represent the original and the updated versions of the private key PRk (page 7, last paragraph). Asanoma reference discloses several embodiments, and whereas a first embodiment utilizes only one private key (fig. 3), a second embodiment permits use of more than one private key (i.e., the smart card initially stores PRk1 and PRk2, and when its memory space becomes insufficient, the smart card moves PRk2 to the hard disk of the user terminal in order to make room for PRk3) (figures 9-10, paragraphs 84, 88-89).

Applicant argues that, in Chen, the second ciphering key (i.e., the replacement key) is not provided with the rekey request (page 8, third paragraph). Chen is not relied upon for the teaching of providing the replacement key with the rekey request; that feature is already disclosed by Asanoma.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 21-23 are rejected under 35 U.S.C. 101 because the claims are directed to non-statutory subject matter. Regarding claim 21, it is not tangibly embodied as it is only software per se. Claim 21 is directed to an apparatus; however, (i) none of the claimed elements is a physical part of a device (e.g., a processor, memory, etc.) can the apparatus as claimed constitute part of a device or a combination of devices to be a machine within the meaning of 101, and (ii) all elements of the claim can be reasonably interpreted in light of the disclosure by one of ordinary skill as software routines (page 8, lines 20-22). Therefore, the claim is directed to software per se, which fails to fall within one of the four statutory classes of § 101.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 14-16, 18-21 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma et al. (2003/0056099) in view of Chen et al. (7,099,476). Asanoma discloses a method and apparatus for updating a private key in a smart card containing multiple private keys (Abstract; figures 5, 9-10). Chen discloses a method for updating a ciphering key including the steps for verifying that a correct key has been updated (Abstract; fig. 2, steps 220-250).

Regarding claims 1-6, 16, 18-21 and 25-26, Asanoma discloses a method and apparatus for secure replacement of a private key in a smart card containing multiple private keys, comprising: receiving a rekey request including an encrypted replacement private key (fig. 7, step 22); authenticating the rekey request (i.e., decrypting the encrypted replacement private key using a key shared with a central system) (fig. 7, step 25); replacing the private key with the replacement private key (fig. 7, step 25). Asanoma does not explicitly disclose that the rekey request identifies a private key for replacement; however, this feature is deemed to be inherent to Asanoma method because figures 5 and 9-10 and paragraphs 84, 88-89 show that the smart card stores multiple private keys. The smart card would not know which key among the stored private keys to be updated if the request did not include the identifier of the key to be updated.

Asanoma does not disclose sending a challenge to the smart card where a key is to be updated, encrypting the challenge with the new/updated key, and returning the encrypted challenge. Chen discloses a method for updating a ciphering key at a node including sending a challenge to the node where a key is to be updated, encrypting the challenge with the new/updated key, and returning the encrypted challenge (fig. 2, steps 220-250). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Asanoma's method to include the steps of sending a challenge to the smart card where a private key is to be updated, encrypting the challenge with the updated private key, and returning the encrypted challenge, as taught by Chen. The motivation for doing so would have been to confirm that a correct key has been updated (col. 6, lines 46-49). Accordingly, the challenge is included in the request to reduce transmission overhead.

Regarding claims 14-15, Asanoma does not disclose that the private key is used to access a document, to perform on-line banking/purchasing or to view a Web site content. Official Notice is taken that both concept and advantage of using public key infrastructure (PKI) in different fields including content access and/or on-line transactions are well known and expected in the art. It would have been obvious to use the private key in different fields

including content access and/or on-line transactions as the PKI is known for providing better security and easier key management.

8. Claims 7-8, 17, 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claims 1, 16 and 21 above, and further in view of Shambroom (6,198,824). Asanoma does not disclose that the rekey request includes a time stamp. Shambroom discloses including a timestamp in a message to restrict replay attacks (col. 8, lines 4-10). It would have been obvious to modify the combined method of Asanoma and Chen to include a time stamp in the rekey request, as taught by Shambroom, in order to restrict replay attack (col. 8, lines 4-10).

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma, Chen and Shambroom as applied to claim 8 above, and further in view of Morimoto (7,024,553). Asanoma, Chen and Shambroom do not disclose a time limit for rekeying. Morimoto discloses a method for updating encryption keys wherein the time limit for rekeying is one day or more depending on system requirements (col. 12, lines 15-26). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Asanoma, Chen and Shambroom to

set the time limit for rekeying to one day or more, as taught by Morimoto, in order to meet the system requirements.

10. Claims 11-12 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claims 1 and 25 above, and further in view of Appenzeller et al. (6,886,096). Asanoma discloses receiving the rekey request from a key generator (fig. 3, element 11) which is separate from a certificate authority (fig. 3, element 22). Appenzeller discloses that a key generator and a certificate authority can be combined into one entity (col. 21, lines 18-24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Asanoma and Chen to combine the key generator and the certificate authority into one entity, as taught by Appenzeller. The motivation for doing so would have been to reduce network traffic communicated between them.

11. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claim 1 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography"). Asanoma does not disclose signing the rekey request and verifying the corresponding signature. Menezes discloses signing a message containing key information and

verifying the signature of the message by the receiver (page 509, Section 12.5.2, first paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Asanoma and Chen to sign the rekey request and verifying the corresponding signature, as taught by Menezes. The motivation for doing so would have been to provide source authentication (page 509, Section 12.5.2, first paragraph).

Allowable Subject Matter

12. Claims 10 and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

13. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 10, the limitation "storing key identifiers of previously deleted keys in memory; reading a key identifier of the private key; comparing the read key identifier to key identifiers of previously deleted private keys; and rejecting the key request if the read key identifier matches any of the key identifiers of previously deleted keys", in combination with elements of the parent claims, have not been taught by prior art. Claim 24 is an apparatus claim corresponding to claim 10.

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

01/09/08

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100